UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,328	03/06/2002	David A. Carlson	005655.P007	9037

8791 7590 09/06/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/092,328	**Applicant(s)** CARLSON, DAVID A.	
	Examiner David G. Cervetti	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-8,11-13,15-21,23-30,32,35-39 and 42-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-8,11-13,15-21,23-30,32,35-39 and 42-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed Jun 21, 2006, have been fully considered.

2. Claims 1,4-8, 11-13, 15-21, 23-30, 32, 35-39, 42-44 are pending and have been examined. Claims 2, 3, 9, 10, 14, 22, 31, 33, 34, 40, and 41 have been canceled.

Response to Amendment

3. The objection to the specification is withdrawn.

4. Applicant's arguments have been fully considered but are moot in view of the new ground(s) of rejection.

5. The instant application applies the technique of speculative execution, which combines dynamic scheduling with branch prediction, and was conventional and well known technique at the time the invention was made, to the encryption field.

6. Speculative execution, as someone of ordinary skill in the art would promptly recognize, calls for re-executing the instructions should a miss-prediction occur.

7. The fact that the instant application recites cipher operations/instructions is not persuasive, since the processors use speculative execution techniques to "**execute instructions**" regardless of what type of instructions. Using a processor that uses speculative execution to implement a conventional and well known encryption algorithm is not patentably different from a processor that uses speculative execution. The fact that the instant application is implementing RC4 using speculative execution techniques is not persuasive, since it simply executes the different operations already taking place in the RC4 algorithm using an speculative execution technique. Applicant's arguments are not persuasive.

Continued Examination Under 37 CFR 1.114

8. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

Claim Rejections - 35 USC § 101

9. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. Claims 1, 4-6, 8, 13, 15-17, 20, 32, 35-37, and 39 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1, 8, 13, 32 recite no practical result, but an intermediate operation.

Claims 4-6 are rejected based on their dependency from claim 1.

Claims 15-17 and 20 are rejected based on their dependency from claim 13.

Claims 35-37 are rejected based on their dependency from claim 32.

Claims 7, and 11-12, 18-19, 38, 42-44 are objected to, but would overcome the 101 issues if rewritten to include all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 103

11. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

12. Claims are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldberg et al. (NPL "Architectural Consideration for Cryptanalytic Hardware", hereinafter Goldberg)

Regarding claims 1 and 32, Goldberg teaches

- receiving a data cipher operation (pages 8-11);
- processing the data cipher operation, wherein the processing comprises generating a number of portions of ciphertext from plaintext, wherein a load operation associated with the generating of at least one portion of the ciphertext executes prior to a store operation associated with the generating of a prior portion of the ciphertext, wherein the generating of the at least one portion of the ciphertext and the generating of the prior portion of the ciphertext is executed within one iteration of a number of iterations for the data cipher operation, and wherein the generating of the at least one portion of the ciphertext is re-executed in an iteration that is subsequent to the one iteration upon determining that data retrieved from the load operation conflicts with data stored in the store operation (pages 8-11).

Goldberg does not expressly disclose using speculative execution techniques with the RC4 encryption algorithm, but uses them with the DES algorithm.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply the teachings of Goldberg regarding DES to other encryption algorithms. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use speculative execution of instructions.

Regarding claims 4 and 35, Goldberg teaches wherein the store operation comprises swapping data within a data structure, the data within the data structure used in generating the ciphertext (pages 8-11).

Regarding claims 5 and 36, Goldberg teaches wherein the load operation comprises accessing data from the data structure (pages 8-11).

Regarding claims 6 and 37, Goldberg teaches wherein the generating of the at least one portion of the ciphertext is aborted upon determining that the data being swapped equals the data being accessed in the data structure (pages 8-11).

Regarding claims 7 and 38, Goldberg teaches wherein the data cipher operation comprises an RC4 operation and wherein the data structure comprises a substitution-box (pages 8-11).

Regarding claims 8 and 39, Goldberg teaches

- receiving a request to perform for data ciphering of plaintext (pages 8-11); and
- processing the request based on a data structure stored in a memory coupled to the processor, wherein the processing comprises, performing a first access of data from the data structure (pages 8-11);

- swapping the data from the first access;
- data ciphering a first portion of the plaintext based on the swapped data from the first access;
- performing a second access of data from the data structure prior to the swapping of the data from the first access;
- performing the following, upon determining that the data from the first access does not equal the data from the second access, swapping the data from the second access; and
- data ciphering a second portion of the plaintext based on the swapped data from the second access in an iteration including data ciphering a first portion of the plaintext based on the swapped data from the first access; and
- performing the following, upon determining that the data from the first access equals data from the second access, re-executing the performing of the second access of data from the data structure in an iteration that is subsequent to determining that the data from the first access does not equal the data from the second access;
- swapping the data from the second access (pages 8-11); and
- data ciphering the second portion of the plaintext based on the swapped data from the second access (pages 8-11).

Goldberg does not expressly disclose using speculative execution techniques with the RC4 encryption algorithm, but uses them with the DES algorithm.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply the teachings of Goldberg regarding DES to other encryption algorithms. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use speculative execution of instructions.

Regarding claims 11 and 42, Goldberg teaches wherein the data ciphering comprises an RC4 operation (pages 8-11).

Regarding claims 12 and 43, Goldberg teaches wherein the data structure comprises a substitution-box (pages 8-11).

Regarding claim 13, Goldberg teaches an apparatus comprising:

- a memory to store a data structure (pages 8-11); and
- a processing unit coupled to the memory, the processing unit to execute a data ciphering operation, wherein the processing unit is to swap data stored in the data structure for data ciphering of a first portion of plaintext, wherein, prior to the completion of the swapping of the data stored in the data structure for data ciphering of the first portion of the plaintext, the processing unit is to access data stored in the data structure for data ciphering of a second portion of the plaintext, and wherein the processing unit is to data cipher the second portion of the plaintext upon determining that the data being swapped in the data structure does not equal the data being accessed in the data structure (pages 8-11).

Goldberg does not expressly disclose using speculative execution techniques with the RC4 encryption algorithm, but uses them with the DES algorithm.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply the teachings of Goldberg regarding DES to other encryption algorithms. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use speculative execution of instructions.

Regarding claim 15, Goldberg teaches wherein the processing unit is to execute the data ciphering operation across a number of iterations, wherein the swapping of data stored in the data structure for data ciphering of the first portion of plaintext and the accessing of data stored in the data structure for data ciphering of the second portion of the plaintext are executed within one iteration of the number of iterations (pages 8-11).

Regarding claim 16, Goldberg teaches wherein the processing unit is to re-execute, within a subsequent iteration of the number of iterations, the accessing of data stored in the data structure for data ciphering of the second portion of the plaintext, upon determining that the data swapped for data ciphering of the first portion of plaintext equals the data accessed for the data ciphering of the second portion of the plaintext (pages 8-11).

Regarding claim 17, Goldberg teaches wherein the memory is to store the plaintext (pages 8-11).

Regarding claim 18, Goldberg teaches wherein the data ciphering operation comprises an RC4 operation (pages 8-11).

Regarding claim 19, Goldberg teaches wherein the data structure comprises a substitution-box (pages 8-11).

Regarding claim 20, Goldberg teaches wherein the apparatus is coupled to a host processor and a host memory, wherein the processing unit is to receive the data ciphering operation from the host memory (pages 8-11).

Regarding claim 21, Goldberg teaches a co-processor coupled to a host processor and a host memory, the co-processor comprising:

- an interface unit to retrieve a data encryption operation, a substitution (S)-box and plaintext associated with the data encryption operation from the host memory based on an instruction from the host processor (pages 8-11); and
- an execution unit coupled to the interface unit, the execution unit comprising, a memory to store the plaintext and the S-box associated with the operation for the data cipher; a microcontroller unit to schedule the data cipher operation (pages 8-11); and
- a RC4 unit to receive the data cipher operation, wherein the RC4 unit is to swap data stored in the S-box for data ciphering of a first portion of the plaintext wherein the RC4 unit is to read data stored in the S-box for data ciphering of a second portion of the plaintext, prior to completion of the swapping of data stored in the S-box for data ciphering of the first portion of the plaintext, and wherein the RC4 unit is to data cipher the second portion of the plaintext upon determining that the data being swapped in the S-box does not equal the data being read from the S-box (pages 8-11).

Goldberg does not expressly disclose using speculative execution techniques with the RC4 encryption algorithm, but uses them with the DES algorithm.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply the teachings of Goldberg regarding DES to other encryption algorithms. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use speculative execution of instructions.

Regarding claim 21, Goldberg teaches wherein the RC4 unit is to data cipher the first portion of the plaintext (pages 8-11).

Regarding claim 24, Goldberg teaches wherein the RC4 unit is to swap data retrieved from the S-box for the data ciphering of the second portion of the plaintext upon determining that the data being swapped for the data ciphering of the first portion of the plaintext does not equal the data read from the S-box for data ciphering of the second portion of the plaintext (pages 8-11).

Regarding claim 25, Goldberg teaches an apparatus comprising:

- a memory to store a substitution (S)-box;
- an RC4 hardware state machine coupled to the memory to generate a plurality of output text blocks from a plurality of input text blocks, wherein a subset of said plurality of output text blocks are generated as a result of repeating the same sequence of states (pages 8-11), wherein during each of the repeated sequence of states data is speculatively read from said S-box in said memory as part of the generation of a next one of said plurality of output

text blocks prior to a write to said S-box in said memory completing as part of generation of a current one of said plurality of output text blocks (pages 8-11).

Goldberg does not expressly disclose using speculative execution techniques with the RC4 encryption algorithm, but uses them with the DES algorithm.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply the teachings of Goldberg regarding DES to other encryption algorithms. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use speculative execution of instructions.

Regarding claim 26, Goldberg teaches wherein said plurality of output text blocks are ciphertext blocks and said plurality of input text blocks are plaintext blocks (pages 8-11).

Regarding claim 27, Goldberg teaches wherein said plurality of input text blocks are ciphertext blocks and said plurality of output text blocks are plaintext blocks (pages 8-11).

Regarding claim 28, Goldberg teaches a system comprising:

- a host processor;
- a host memory coupled to the host processor, the host memory to include a security operation, wherein the security operation includes a data cipher operation based on RC4, the host memory to include plaintext and a data structure for the data cipher operation (pages 1-6);

- a co-processor coupled to the host processor, the co-processor comprising, an interlace unit to retrieve the security operation from the host memory based on an instruction from the host processor;
- an execution unit coupled to the interlace unit, the execution unit comprising,
- a memory to store the plaintext and the data structure associated with the data cipher operation;
- a microcontroller unit to store the data cipher operation in an execution queue; and
- an RC4 unit coupled to the execution queue, the RC4 unit to receive the data cipher operation, wherein the RC4 unit is to swap data stored in the S-box for data ciphering of a first portion of the plaintext and wherein the RC4 unit is to read data stored in the S-box for data ciphering of a second portion of the plaintext, prior to completion of the swapping of data stored in the S-box for data ciphering of the first portion of the plaintext, and wherein the RC4 unit is to swap data retrieved from the data structure for the data ciphering of the second portion of the plaintext upon determining that the data being swapped for the data ciphering of the first portion of the plaintext does not equal the data read from the data structure for data ciphering of the second portion of the plaintext (pages 8-11).

Goldberg does not expressly disclose using speculative execution techniques with the RC4 encryption algorithm, but uses them with the DES algorithm.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply the teachings of Goldberg regarding DES to other encryption algorithms. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use speculative execution of instructions.

Regarding claim 29, Goldberg teaches wherein the RC4 unit is to data cipher the second portion of the plaintext upon determining that the data being swapped in the data structure does not equal the data being read from the data structure (pages 8-11).

Regarding claim 30, Goldberg teaches wherein the RC4 unit is to data cipher the first portion of the plaintext (pages 8-11).

Regarding claim 44, Goldberg teaches wherein processing the request for data ciphering of the plaintext comprises data ciphering the plaintext over a number of iterations and wherein the data ciphering of the first portion of the plaintext is in a same iteration as the data ciphering of the second portion of the plaintext (pages 8-11).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Favor et al. (US Patents 5,884,059, column 48 and 6,195,744, column 48) teach a processor implementing out-of-order execution of instructions and using it for encryption purposes.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-

5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DGC

NASSER MOAZZAMI
PRIMARY EXAMINER

9/1/06